UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/003,572	10/30/2001	Roger R. Dube	GATEP002	4976

25771 7590 01/13/2005

PATENT VENTURE GROUP
333 N INDIAN HILL BLVD
SUITE 208
CLAREMONT, CA 91711

EXAMINER	
BAUM, RONALD	
ART UNIT	**PAPER NUMBER**
2136	

DATE MAILED: 01/13/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/003,572	DUBE, ROGER R.	
	Examiner	Art Unit	
	Ronald Baum	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-38 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-38 is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This action is in reply to applicant's correspondence of 26 October 2004.

2. Claims 1- 38 are pending for examination.

3. Claims 1- 38 remain rejected.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4. Claims 1-6,15-22,26-33 are rejected under 35 U.S.C. 102(e) as being anticipated by Fischer, U.S. Patent 5,659,617.

5. As per claim 1; "A method for protecting electronic files, comprising:

obtaining environment information regarding a computer, the environment information including data concerning an operating environment of the computer [col. 1,lines 5-col. 4,line 27, whereas environment information regarding a computer clearly deals with its physical location during access (i.e., to files via standard log-in/log-on) via the LCU based certificate aspect];

generating an encryption key based on the environment information [col. 1,lines 5-col. 4,line 27, whereas physical location aspect of the LCU is public key based

(i.e., col. 3,lines 15-col. 4,line 10) because the certificate is public key based (the key certified by virtue of the certificate).]; and

encrypting an electronic file using the encryption key [col. 1,lines 5-col. 4,line 27, whereas the encryption is public key based (the encryption key certified by virtue of the certificate (i.e., col. 2,lines 35-65).].".

6. Claim 2 ***additionally recites*** the limitation that; "A method as recited in claim 1, further comprising the operation of creating a decryption key based on environment information, wherein the decryption key can be utilized to decrypt the electronic file.". The teachings of Fischer suggest such limitations (col. 1,lines 5-col. 4,line 27, whereas the encryption and associated decryption is public key based (the encryption key certified by virtue of the certificate (i.e., col. 2,lines 35-65) which is certified to assure proper association of the public (i.e., encryption) and private (i.e., decryption) keys in public key based cryptographic functionality.).

7. Claim 3 ***additionally recites*** the limitation that; "A method as recited in claim 2, wherein the encryption key and the decryption key are public key infrastructure (PKI) based keys.". The teachings of Fischer suggest such limitations (col. 1,lines 5-col. 4,line 27, whereas the encryption and associated decryption is public key based (the encryption key certified by virtue of the certificate (i.e., col. 2,lines 35-65) which is certified to assure proper association of the public (i.e., encryption) and private (i.e., decryption) keys in public key based cryptographic functionality.).

8. Claim 4 ***additionally recites*** the limitation that; "A method as recited in claim 1, wherein the environment information includes location information of the computer.". The teachings of Fischer suggest such limitations (col. 1,lines 5-col. 4,line 27, whereas environment information

regarding a computer clearly deals with its physical location during access (i.e., to files via standard log-in/log-on) via the LCU based certificate aspect.).

9. Claim 5 ***additionally recites*** the limitation that; "A method as recited in claim 4, wherein the location information specifies a location of the computer within a predetermined range.". The teachings of Fischer suggest such limitations (col. 1,lines 5-col. 4,line 27, whereas environment information regarding physical location via the LCU based certificate aspect is such that the GPS accuracy and inherent tolerance of timing (i.e., col. 5,lines 9-col. 9,line 31, beacon/clock timing) errors clearly allows for the location information specifies a location of the computer within a predetermined range.).

10. Claim 6 ***additionally recites*** the limitation that; "A method as recited in claim 5, wherein the location information is provided by global positioning satellite (GPS) data.". The teachings of Fischer suggest such limitations (col. 1,lines 5-col. 4,line 27, whereas environment information regarding physical location via the LCU based certificate aspect is GPS based.).

11. As per claim 15; "A method for protecting electronic files, comprising:

storing an electronic file encrypted using an encryption key,

wherein the encryption key is generated using a first environment profile of a computer, and

wherein the environment profile includes data concerning an operating environment of the computer [col. 1,lines 5-col. 4,line 27, whereas environment information regarding a computer clearly deals with its physical location during access (i.e., to encrypted and clearly stored files via standard log-in/log-on) via the LCU based certificate aspect. Further,

the physical location aspect of the LCU is public key based (i.e., col. 3,lines 15-col. 4,line 10) because the certificate is public key based (the key certified by virtue of the certificate), and the encryption is public key based (the encryption key certified by virtue of the certificate (i.e., col. 2,lines 35-65).];

obtaining a second environment profile of the computer based on a current operating environment of the computer [col. 1,lines 5-col. 4,line 27, whereas environment information regarding a computer clearly deals with its physical location during access (i.e., during second operating environment of the computer data collection for the purpose of comparison of profile information for the explicit purpose of file access of to encrypted and clearly stored files via standard log-in/log-on) via the LCU based certificate aspect];

generating a decryption key based on the second environment profile; and

decrypting the electronic file using the decryption key [col. 1,lines 5-col. 4,line 27, whereas the encryption and associated decryption is public key based (the encryption key certified by virtue of the certificate (i.e., col. 2,lines 35-65) which is certified to assure proper association of the public (i.e., encryption) and private (i.e., decryption) keys in public key based cryptographic functionality.].".

12. Claim 16 ***additionally recites*** the limitation that; "A method as recited in claim 15, wherein the encryption key and the decryption key are further based on a passcode received from a user.". The teachings of Fischer suggest such limitations (col. 1,lines 5-col. 4,line 27, whereas the public key based encryption key certified by virtue of the certificate (i.e., col. 2,lines 35-65),

and further layered access control derived from using said certificate, is associated with the use of PIN/password functionality for the LCU (i.e., col. 3,lines 63-col. 4,line 10, col. 10,lines 45-col. 11,line 5).).

13. Claim 17 ***additionally recites*** the limitation that; "A method as recited in claim 16, further comprising the operation of appending the first environment profile to the passcode to generate the encryption key.". The teachings of Fischer suggest such limitations (col. 1,lines 5-col. 4,line 27, whereas the public key based encryption key certified by virtue of the certificate (i.e., col. 2,lines 35-65), and further layered access control derived from using said certificate, is associated with the use of PIN/password functionality for the LCU (i.e., col. 3,lines 63-col. 4,line 10, col. 10,lines 45-col. 11,line 5).).

14. Claim 18 ***additionally recites*** the limitation that; "A method as recited in claim 17, further comprising the operation of appending the current environment profile to the passcode to generate the decryption key.". The teachings of Fischer suggest such limitations (col. 1,lines 5-col. 4,line 27, whereas the public key based encryption key certified by virtue of the certificate (i.e., col. 2,lines 35-65), and further layered access control derived from using said certificate, is associated with the use of PIN/password functionality for the LCU (i.e., col. 3,lines 63-col. 4,line 10, col. 10,lines 45-col. 11,line 5).).

15. Claim 19 ***additionally recites*** the limitation that; "A method as recited in claim 18, wherein the decryption key cannot decrypt the electronic file when the current environment profile does not match the first environment profile.". The teachings of Fischer suggest such limitations (col. 1,lines 5-col. 4,line 27, whereas the public key based encryption key certified by virtue of the certificate (i.e., col. 2,lines 35-65), and further layered access control derived from

using said certificate, is associated with the use of PIN/password functionality for the LCU (i.e., col. 3,lines 63-col. 4,line 10, col. 10,lines 45-col. 11,line 5).).

16. Claim 20 ***additionally recites*** the limitation that; "A method as recited in claim 19, wherein a match occurs when the data in the current environment profile is within a predetermined range of the data in the first environment profile.". The teachings of Fischer suggest such limitations (col. 1,lines 5-col. 4,line 27, whereas the public key based encryption key certified by virtue of the certificate (i.e., col. 2,lines 35-65), and further layered access control derived from using said certificate, is associated with the use of PIN/password functionality for the LCU (i.e., col. 3,lines 63-col. 4,line 10, col. 10,lines 45-col. 11,line 5). Further, whereas the aspect of the environment information regarding physical location via the LCU based certificate is such that the GPS accuracy and inherent tolerance of timing (i.e., col. 5,lines 9-col. 9,line 31, beacon/clock timing) errors clearly allows for the location information specifies a location of the computer within a predetermined range.).

17. Claim 21 ***additionally recites*** the limitation that; "A method as recited in claim 15, wherein the environment profile includes location information specifying a location of the computer within a predetermined range.". The teachings of Fischer suggest such limitations (col. 1,lines 5-col. 4,line 27, whereas environment information regarding physical location via the LCU based certificate aspect is such that the GPS accuracy and inherent tolerance of timing (i.e., col. 5,lines 9-col. 9,line 31, beacon/clock timing) errors clearly allows for the location information specifies a location of the computer within a predetermined range.).

18. Claim 22 ***additionally recites*** the limitation that; "A method as recited in claim 21, wherein the location information is provided by global positioning satellite (GPS) data.". The

teachings of Fischer suggest such limitations (col. 1,lines 5-col. 4,line 27, whereas environment information regarding physical location via the LCU based certificate aspect is GPS based.).

19. As per claim 26; "A method for protecting electronic files comprising;

authenticating a digital transaction using a delay number based on a timing signal received from a remote source [col. 1,lines 5-col. 4,line 27, whereas environment information regarding a computers physical location as a function of GPS (i.e., col. 2,lines 3-19, col. 4,lines 27-col. 5,line 22) via the LCU based certificate clearly uses remote source (GPS satellite transmission) to LCU (receiving said transmission) as a delay number based on a timing signal.];

obtaining environment information regarding a computer, the environment information including data concerning an operating environment of the computer [col. 1,lines 5-col. 4,line 27, whereas environment information regarding a computer clearly deals with its physical location during access (i.e., to files via standard log-in/log-on) via the LCU based certificate aspect];

generating an encryption key based on the environment information [col. 1,lines 5-col. 4,line 27, whereas physical location aspect of the LCU is public key based (i.e., col. 3,lines 15-col. 4,line 10) because the certificate is public key based (the key certified by virtue of the certificate).]; and

encrypting an electronic file using the encryption key [col. 1,lines 5-col. 4,line 27, whereas the encryption is public key based (the encryption key certified by virtue of the certificate (i.e., col. 2,lines 35-65).].".

20. Claim 27 ***additionally recites*** the limitation that; "A method as recited in claim 26, wherein the delay number is based on a delay time period between when the timing signal was transmitted and when the timing signal was received.". The teachings of Fischer suggest such limitations (col. 1,lines 5-col. 4,line 27, whereas environment information regarding a computers physical location as a function of GPS (i.e., col. 2,lines 3-19, col. 4,lines 27-col. 5,line 22) via the LCU based certificate clearly uses remote source (GPS satellite transmission) to LCU (receiving said transmission) as a delay number based on a timing signal.).

21. Claim 28 ***additionally recites*** the limitation that; "A method as recited in claim 27, wherein the delay in the timing signal is caused by free electrons in a line of sight between the remote source and a receiver.". The teachings of Fischer suggest such limitations (col. 1,lines 5-col. 4,line 27, whereas environment information regarding a computers physical location as a function of GPS (i.e., col. 2,lines 3-19, col. 4,lines 27-col. 5,line 22) via the LCU based certificate clearly uses remote source (GPS satellite transmission) to LCU (receiving said transmission) and the delay in the timing signal is inherently a timing aspect caused by free electrons in a line of sight between the remote source and a receiver.).

22. Claim 29 ***additionally recites*** the limitation that; "A method as recited in claim 28, wherein the delay in the timing signal is further caused by variations in atmospheric conditions.". The teachings of Fischer suggest such limitations (col. 1,lines 5-col. 4,line 27, whereas for GPS using remote source (GPS satellite transmission) to LCU (receiving said transmission) delay in the timing signal is inherently a timing aspect further caused by the variations in atmospheric conditions.).

23. Claim 30 ***additionally recites*** the limitation that; "A method as recited in claim 26, further comprising the operation of creating a decryption key based on environment information, wherein the decryption key can be utilized to decrypt the electronic file.". The teachings of Fischer suggest such limitations (col. 1,lines 5-col. 4,line 27, whereas the encryption and associated decryption is public key based (the encryption key certified by virtue of the certificate (i.e., col. 2,lines 35-65) which is certified to assure proper association of the public (i.e., encryption) and private (i.e., decryption) keys in public key based cryptographic functionality.).

24. Claim 31 ***additionally recites*** the limitation that; "A method as recited in claim 30, wherein the encryption key and the decryption key are public key infrastructure (PKI) based keys.". The teachings of Fischer suggest such limitations (col. 1,lines 5-col. 4,line 27, whereas the encryption and associated decryption is public key based (the encryption key certified by virtue of the certificate (i.e., col. 2,lines 35-65) which is certified to assure proper association of the public (i.e., encryption) and private (i.e., decryption) keys in public key based cryptographic functionality.).

25. Claim 32 ***additionally recites*** the limitation that; "A method as recited in claim 26, wherein the environment information includes location information specifying a location of the computer within a predetermined range.". The teachings of Fischer suggest such limitations (col. 1,lines 5-col. 4,line 27, whereas environment information regarding physical location via the LCU based certificate aspect is such that the GPS accuracy and inherent tolerance of timing (i.e., col. 5,lines 9-col. 9,line 31, beacon/clock timing) errors clearly allows for the location information specifies a location of the computer within a predetermined range.).

26. Claim 33 ***additionally recites*** the limitation that; "A method as recited in claim 32, wherein the location information is provided by global positioning satellite (GPS) data.". The teachings of Fischer suggest such limitations (col. 1,lines 5-col. 4,line 27, whereas environment information regarding physical location via the LCU based certificate aspect is GPS based.).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

27. Claims 7-9,23,34 are rejected under 35 U.S.C. 103(a) as being unpatentable over Fischer, U.S. Patent 5,659,617 as applied to claims 1,15,26 respectively, above, and further in view of Overfield, U.S. Patent 5,598,577.

Claim 7 ***additionally recites*** the limitation that; "A method as recited in claim 1, wherein the environment information includes drive information regarding a drive wherein the electronic file will be stored.";

Claim 8 ***additionally recites*** the limitation that; "A method as recited in claim 7, wherein the drive information includes a drive identifier that identities the particular drive wherein the electronic file will be stored.";

Claim 9 ***additionally recites*** the limitation that; "A method as recited in claim 7, wherein the drive information includes an electronic address assignment of the particular drive wherein the electronic file will be stored.";

Claim 23 ***additionally recites*** the limitation that; "A method as recited in claim 15, wherein the environment information includes drive information regarding a drive wherein the electronic file will be stored.";

Claim 34 ***additionally recites*** the limitation that; "A method as recited in claim 26, wherein the environment information includes drive information regarding a drive wherein the electronic file will be stored.".

The teachings of Fischer suggest base claims ("A method for protecting electronic files, comprising: obtaining environment information regarding a computer, the environment information including data concerning an operating, environment of the computer...") limitations (Abstract, col. 1,lines 5-col. 4,line 27, col. 5,lines 9-col. 9,line 31) *without explicitly teaching* of the use of "environment information includes drive information [including 'electronic address assignment'] regarding a drive wherein the electronic file will be stored".

Overfield teaches of using; "[system software] queries a disk drive to determine its model. The system software checks the corresponding response string with reference to a table of recognized model strings (in encrypted format). If the drive's response string is recognized in this table, then the drive parameters can be set appropriately. [Abstract, col. 1,lines 32-col. 4,line 45]" Such that "the corresponding response string" clearly corresponds to drive information (including "electronic address assignment").

Thus, it would have been obvious to a person of ordinary skill in the art at the time of the invention to have been motivated to combine the Overfield disk drive querie/response parameter authentication and authorization invention, to the Fischer method/system protecting electronic files via obtaining environment information (location certificate based) regarding a computer.

Such motivation to combine would clearly encompass the need to allow for qualitatively superior authentication scenario to improve security in a disk file configured computer system, whereas the authentication and authorization for file access (i.e., disk drive specific via drive configuration) clearly is a function of said disk drive querie/response parameters. (i.e., col. 9,line 62-col. 10,line 54).

28. Claims 10-14,24-25,35-38 are rejected under 35 U.S.C. 103(a) as being unpatentable over Fischer, U.S. Patent 5,659,617 as applied to claims 1,15,26 respectively, above, and further in view of Schneck et al, U.S. Patent 5,933,498.

Claim 10 ***additionally recites*** the limitation that; "A method as recited in claim 1, wherein the environment information includes time information specifying access duration.";

Claim 11 ***additionally recites*** the limitation that; "A method as recited in claim 10, wherein the access duration is a time range indicating a time period when the electronic file can be accessed.";

Claim 12 ***additionally recites*** the limitation that; "A method as recited in claim 11, wherein the electronic file cannot be decrypted at a time outside the time range.";

Claim 13 ***additionally recites*** the limitation that; "A method as recited in claim 10, wherein the access duration is a date range indicating a range of dates when the electronic file can be accessed.";

Claim 14 ***additionally recites*** the limitation that; "A method as recited in claim 13, wherein the electronic file cannot be decrypted at a date outside the date range.";

Claim 24 ***additionally recites*** the limitation that; "A method as recited it claim 15, vvherein the environment information includes time information specifying access duration, wherein the access duration is a time range indicating a tine period when the electronic file can be accessed.";

Claim 25 ***additionally recites*** the limitation that; "A method as recited it claim 15, wherein the environment information includes date information specifying access duration, wherein the access duration is a date range indicating dates that the electronic file can be accessed.";

Claim 35 ***additionally recites*** the limitation that; "A method as recited in claim 26, wherein the environment information includes time information specifying access duration, wherein the access duration is a time range indicating a time period when the electronic file can be accessed.";

Claim 36 ***additionally recites*** the limitation that; "A method as recited in claim 35, wherein the electronic file cannot be decrypted at a time outside the time range.";

Claim 37 ***additionally recites*** the limitation that; "A method as recited in claim 26, wherein the environment information includes date information specifying access duration, wherein the access duration is a date range indicating dates that the electronic file can be accessed.";

Claim 38 ***additionally recites*** the limitation that; "A method as recited in claim 37, wherein the electronic file cannot be decrypted on a date outside the date range.".

The teachings of Fischer suggest base claims ("A method for protecting electronic files, comprising: obtaining environment information regarding a computer, the environment

information including data concerning an operating, environment of the computer...") limitations (Abstract, col. 1,lines 5-col. 4,line 27, col. 5,lines 9-col. 9,line 31) *without explicitly teaching* of the use of "time [and date] range indicating a time period [and date period] when the electronic file can [and can't] be accessed [decrypted]".

Schneck et al teaches of using; "A method and device are provided for controlling access to data. Portions of the data are protected and rules concerning access rights to the data are determined. Access to the protected portions of the data is prevented, other than in a non-useable form; and users are provided access to the data only in accordance with the rules as enforced by a mechanism protected by tamper detection. A method is also provided for distributing data for subsequent controlled use of those data. The method includes protecting portions of the data; reventing access to the protected portions of the data other than in a non-useable form; determining rules concerning access rights to the data; protecting the rules...[Abstract], and further; "The invention can restrict the qualities or quantities of access to data in any manner that can be calculated or enumerated. A non-exhaustive, representative set of examples is given below..." [col. 25,lines 6-col. 27,line 27]" such that "the non-exhaustive, representative set of examples is given below...[list]" clearly corresponds to "time [and date] range indicating a time period [and date period] when the electronic file can [and can't] be accessed [decrypted]" via the specific policy creation as used for the said encryption/decryption and access control funtionality.

Thus, it would have been obvious to a person of ordinary skill in the art at the time of the invention to have been motivated to combine the Schneck et al policy based access control

invention, to the Fischer method/system protecting electronic files via obtaining environment information (location certificate based) regarding a computer.

Such motivation to combine would clearly encompass the need to allow for qualitatively superior authentication scenario to improve security in a disk file configured computer system, whereas the authentication and authorization for file access (i.e., disk drive specific via drive configuration) clearly is a function of said disk drive policy access time, date, etc., criteria. (i.e., Abstract, col. 6,line 49-col. 8,line 47, col. 25,lines 6-col. 27,line 27).

Response to Amendment

29. As per applicant's argument concerning the lack of teaching (for independent claims 1,15 and 26 specifically) by Fischer of "generating an encryption key based on environment information ...", the examiner has fully considered the arguments and finds them not to be persuasive. The use of the "multiple levels of certification... to chain through the certification hierarchy to ... determine ... public key ... associated with a trusted LCU." (i.e., see col. 3,lines 50-62) clearly encompasses the key generation as a function of environment (i.e., the location and/or LCU memory parameters) as broadly interpreted by the examiner, in that the chaining per se, as applied to the signing/authentication aspects of encryption, encompasses the recursive functionality of 'previous data (i.e., the location/keying data)' with a key inherently a function of the previous data. Further, the use of "conventional safeguards ... PIN ... password ..." (i.e., col. 3,lines 63-col. 4,line 27), clearly is associated with securing access to data via information encryption, in itself associated with the key used thereof, which further deals with the claim language limitations broadly associated with keying/activation as related to the data protection

(i.e., encryption via a key of a file, consisting of data, such as a digital certificate per se). Still further, the location and time tagged aspects of the beacon embodiments (i.e., col. 4,lines 11-27), clearly deal with the location/key aspects of the claim language.

The *claim language* specifically dealing with the phrase '...generating an encryption key based on the environment information ... and ... encrypting an electronic file ...', is sufficiently broad such that the Fischer aspects of the referenced location authentication/verification/certification system/methods, would therefore be applicable in the rejection, such that the rejection support references collectively encompass the said claim limitations in their entirety.

30. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Conclusion

31. Any inquiry concerning this communication or earlier communications from examiner should be directed to Ronald Baum, whose telephone number is (571) 272-3681, and whose unofficial Fax number is (571) 273-3681. The examiner can normally be reached Monday through Friday from 8:00 AM to 5:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh, can be reached at (571) 272-3795. The Fax number for the organization where this application is assigned is 703-872-9306.

Ronald Baum

Patent Examiner

E. Moise

EMMANUEL L. MOISE
PRIMARY EXAMINER